Exhibit 3

CSO

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO

MAR 6, 2017 4:00 AM PT

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Spammers expose their entire operation through bad backups

Faulty Rsync setup exposes River City Media's entire operation, group is one of Spamhaus' top offenders (infographic)

This is the story of how River City Media (RCM), Alvin Slocombe, and Matt Ferris, accidentally exposed their entire operation to the public after failing to properly configure their Rsync backups.

The data from this well-known, but slippery spamming operation, was discovered by Chris Vickery, a security researcher for MacKeeper and shared with Salted Hash, Spamhaus, as well as relevant law enforcement agencies.

While security practitioners are familiar with spammers and their methods, this story afforded Salted Hash with a rare opportunity to look behind the curtain and view their day-to-day operations.

■ **RELATED: How can you detect a fake ransom letter?**

Something's not right:

"If you have not changed your Skype and Hipchat passwords as yet, please do so ASAP," wrote Alvin Slocombe in early February on HipChat.

He suspected the company had been hacked. In his all-staff message, he urged everyone to rotate passwords for "anything that we may have stored any information on in the past."

The assumptions were wrong though.The company wasn't hacked. Yet, the reality is, RCM still experienced a severe data breach - one they were directly responsible for. By this point, their backups had been exposed for more than a month.

Vickery had discovered everything. From Hipchat logs and domain registration records, to accounting details, infrastructure planning and production notes, scripts, and business affiliations. In addition, Vickery uncovered 1.34 billion email accounts. These are the accounts that will receive spam, or what RCM calls offers. Some of these records also contained personal information, such as full names, physical addresses, and IP addresses.

"The natural response is to question whether the data set is real," Vickery explained in his notes on the discovery.

"That was my initial reaction. I'm still struggling with the best software solution to handle such a voluminous collection, but I have looked up several people that I know and the entries are accurate. The only saving grace is that some are outdated by a few years and the subject no longer lives at the same location."

Vickery also discovered thousands of warm-up email accounts used by RCM to skirt anti-spam measures. As a whole, most of the personal records and email addresses he discovered were collected by a process called co-registration, or CoReg.

CoReg emails come from people who signed-up for something online, and had their address shared with a third-party or partner.

"Nobody would knowingly give their email address to spammers, so they have to be tricked into it. Usually, there is some kind of offer for a 'free gift' in exchange for giving up an email address and personal information. The fine print of these offers allows the company to share their address with their 'partners' which ends up also being their partner's partners, and their partner's partner's partners, until every spammer on the planet has their address," explained Spamhaus' Mike Anderson.

Partial list of alleged opt-in addresses

He goes on to explain such address lists are the lifeblood of the industry, and they're constantly being analyzed through tracking systems - examining which addresses are viewing spam ads, which ones are clicking on them, and which ones are buying.

"Meanwhile, the original contract for handing over the address is never fulfilled, since it turns out to be impossible to redeem the 'free gift' or only with extreme difficulty. And of course these addresses never go through a confirmation process, to ensure it's the real owner of the address doing the signup."

For this story, we'll explore the finances and operations of RCM, but it is important to note the data is only a snapshot taken from backups. Many of the records are current as of January, 2017, while others were last updated in December of 2016.

After seeing some of the documents, and spending countless days explaining how things work with both Salted Hash and Vickery, Spamhaus concluded that RCM has been using illegal IP hijacking techniques during some of their campaigns.

Law enforcement was informed about the breach and the questionable activities it exposed. However, we cannot discuss those elements, because the agencies involved cannot comment on pending or ongoing investigations.

For their part, Spamhaus will be taking action on all of the IP addresses and other elements connected to abuse stemming from this incident. The problem is, organizations like River City Media use numerous aliases and affiliate programs, so while blocking their infrastructure will hurt, there is no assurance it will put them out of business for good.

Update: With regard to notification, Vickery said he didn't reach out to RCM directly.

> *"Once we concluded that this was indeed related to a criminal operation, it was decided that we should approach law enforcement and the affected companies (like Microsoft and Yahoo) before making any attempts at contacting the spammers directly. The leaking servers went dark during the process of notifying law enforcement and the major companies. So, I did not directly contact the spammers themselves."*

River City Media, a Top 10 ROKSO operation:

The Register of Known Spam Operations (ROKSO) database is maintained by Spamhaus, an organization dedicated to fighting spam. ROKSO tracks professional spam operations and lists them using a three-strike rule. Listed among dozens of operators on the database's index is Alvin Slocombe, the owner of Cyber World Internet Services, Inc.

Slocombe is also connected to a few other aliases, including e-Insites, Brand 4 Marketing, Ad Media Plus, and Site Traffic Network. He's often associated with Matt Ferris, and his company River City Media. In all, the documents exposed by

RCM connect the organization to more than 20 business partners over the last two years, and more than 30 different aliases, including RCM Delivery, Pheasant Valley Marketing Group, eBox, and Wharton Dynamics, Inc.

A brief overview of RCM's operations.

Moreover, RCM's data breach also exposed 2,199 IP addresses used for public-faced activities; as well as the group's internal assets. This is in addition to the 60 IP blocks RCM has identified for activities in the past, as well as current and future operations; and the 140 active DNS servers that are rotated frequently.

Based on campaign logging documents, the data breach also exposed more than 300 active MX records. In just two spreadsheets alone, RCM recorded nearly 100,000 domains used for their campaigns.

As mentioned, Vickery discovered tens of thousands of email accounts used for warm-up. These warm-up accounts are computer generated and maintained by RCM staff. Their usage and creation almost certainly violates the terms of service (TOS) at the large email providers where they were created. The exposed RCM records show warm-ups at Gmail, AOL, Hotmail, and Yahoo, but others are sure to exist.

A small example of the domains available to RCM.

The process works like this: RCM will send messages for a given campaign to these warm-up accounts, and since they're not generating complaints from these messages (they're not going to complain about themselves after all), the Email Service Provider or affiliate program will mark them as a good sender. Once they have a solid reputation built-up, they're ready to blast the rest of

the internet with their offers.

If an offer doesn't inbox (meaning it is rejected, or otherwise dumped into a spam or junk folder), or a given domain is blacklisted, RCM goes back to a list of thousands of domains and selects another to restart the process.

In some cases, RCM will use aged domains. Aged domains are valuable, as newly registered domains are immediately suspect – especially if they've never sent email before. Some of the documents exposed by RCM's data breach show plans to purchase aged domains at auction. Other domains purchased in bulk are prepped for warm-up and used once they have a positive age and reputation.

If RCM is caught spamming, the domain being used is dropped and replaced. The process is the same for affiliate IDs. However, Slocombe and Ferris have good relationships with their providers and marketing partners, so there is little risk on their end.

For example: In December of 2016, one of the exposed chat logs shows Slocombe explaining to Ferris that their buddy Mike Boehm is "very close friends with the owner of Alpnames, so if any issues come up let me know and I will see if he can hook us up / not let us get pulled down."

Business Connections:

Alpnames is listed in first place on the Spamhaus list of abused domain registrars. Spamhaus says it now appears as if they prefer to work with spammers, by offering discounts on registrations and assurances that domains won't be canceled for abuse. But Alpnames isn't the only business relationship that stands out, there is also EmailTraffic.com (archive link).

EmailTraffic.com employs Sean McKeown as their Data Management Director, but in RCM chat logs, McKeown is also known as MX. He is the owner of MXLeads in Florida, and he's behind another RCM partner, Fenix Network

In the RCM chat logs, McKeown is respected for his scripting work. His efforts enabled RCM to exploit a number of providers in order to inbox offers. Such examples include Apple (mac, me, iCloud), as well as Hotmail, Gmail, AOL, and more. Salted Hash reached out to all of the providers and shared the scripts and notes exposed by the data breach. As a precaution, we will not be publishing them or releasing details.

The CEO of EmailTraffic.com is Stefan Hansmann, who is also the CEO of Domainers Choice, a company owned by Nanjing Imperiosus Technology Co., Ltd. in China. In 2016, the Executive Office of the President of the United States listed Nanjing Imperiosus Technology Co. as a notorious market for its connection to illegal online pharmacies.

Based on the records exposed by RCM, the company gets a lot of its domains from Domainers Choice, and uses MXLeads or Fenix Network to handle click tracking and unsubscribes. The ties between these companies and RCM is strengthened by the development of Youngstown Systems LLC, which Spamhaus says could be a fake ISP.

Youngstown has MX records on EmailTraffic.com and an A Record pointed to Fenix Network. The exposed documents suggest this ISP was some sort of joint venture between McKeown and RCM, but that might not be the case.

TierPoint logs from River City Media, showing problems inboxing on AOL.

Finally, there is TierPoint, a legitimate ISP with a relationship to Alvin Slocombe and Cyber World Internet Services. They are Cyber World's only link to the rest of the internet. IP records exposed by RCM show Slocombe tracking TierPoint IP addresses while working on various campaigns. Salted Hash reached out to TierPoint, MXLeads, and Domainers Choice for comment, but only TierPoint responded by the time this article

went to press.

In a statement, a Tierpoint spokesperson wouldn't comment on Ferris, Slocombe, River City Media, or Cyber World Internet.

> *"What we can tell you is that we serve more than 5,000 clients; a number of them are hosting companies, and as part of our agreement with some of those companies, we assign a block of IP addresses, which these clients (or their clients) may use. In all cases, if we receive official notice from a law enforcement agency of suspected unlawful activity, spamming or otherwise, we work closely with the agency and take all appropriate steps to protect our larger client base, our facilities, and our network." - Tierpoint*

In addition to the image above, documents exposed by the RCM data breach show an emergency contact at Tierpoint (Dan S.) and a username of *alvinslobombe*. Moreover, engineering chat logs leaked by RCM show Slocombe discussing using Tierpoint servers.

The other business relationships discovered within the exposed RCM documents are central to their operations.

Healthcare records for sale on Dark Web

CSO

SALTED HASH- TOP SECURITY NEWS
By Steve Ragan, Senior Staff Writer, CSO
MAR 6, 2017 4:00 AM PT

About
Fundamental security insight to help you minimize risk and protect your organization

NEWS

Spammers expose their entire operation through bad backups

Faulty Rsync setup exposes River City Media's entire operation, group is one of Spamhaus' top offenders (infographic)

The operations of a Top 10 ROKSO operation:

At its core, RCM is a marketing firm that does email and SMS campaigns. While some of their work is legit, other campaigns ran by the company are questionable to say the least.

Mapped RCM email campaigns, November 2016

When it comes to SMS operations, RCM actually got a client sued over an incident that started in 2011. According to the court, RCM sent unsolicited SMS messages out to an unknown number of phones, triggering complaints almost immediately. One of the people who complained was a lawyer, and he filed a lawsuit.

Recorded campaigns exposed by RCM's data breach include large brands such as Nike, LifeLock, Liberty Mutual, Fidelity, MetLife, Victoria's Secret, Kitchen Aide, Yankee Candle, Bath & Body Works, Gillette, Match.com, Dollar Shave Club, Dewalt, DirecTV, Covergirl, Clinique, Maybelline, Terminix, and AT&T.

Commemorative Trump Coin

RCM has also emailed offers for Trump Coins, oil change coupons, IRS forgiveness, addiction help, offers for new SUVs, ink and toner, veterans loans, blood sugar testing, surgical mesh settlements, metabolism enhancers, cold remedies, survival blankets, and tactical flashlights.

RCM's campaigns are sourced from a number of marketing firms. The largest marketing firm connected to RCM, based on documents exposed by the data breach, public filings, and domain registration records, appears to be Amobee.

Amobee is a display advertiser, meaning they place ads on websites in order to get people to click them. Amobee purchased Adconion Direct in 2014 as a way to boost their display advertising business. The service that enabled Adconion to outsource offers to affiliate companies is called AdDemand.

Setups like this are common, Spamhaus explained. Major brands will turn to advertisers, who then work with affiliates with good reputations. This is why the process of warming-up accounts and domains is critical to the operation.

The documents exposed by RCM's data breach list all of the campaigns the company has worked with AdDemand on, and shows them collecting a payment from Amobee on November 21, 2016 for $72,395.06 for completed work; followed by a payment of $33,979.80 on December 19, 2016.

Each day Amobee will send a complainer's report to RCM, containing the addresses that should stop receiving email, as well as a list of email hashes that should be scrubbed from lists. However, it isn't clear if the removal policy is strictly adhered to.

Examples of offers emailed by RCM

Most of the contracts start off as display advertising, meaning an ad on a website that someone has to click. It's a good bet that many of the major brands represented didn't know their marketing campaigns were being pushed to email. The trick that ties everything together is converting email to display advertising.

"Basically, some affiliate companies are selling display advertising clicks to their customers, but what is hidden from them, much of what's driving these clicks, is simply spam," Spamhaus' Anderson explained.

Several of the links used for a LifeLock campaign eventually landed on a registration page (archive copy) for the service, but the emails look like display ads. In 2015, Cloudmark reported on the LifeLock campaigns (archive link), including one that was similar to the offers RCM was sending earlier that year.

The LifeLock campaign was huge for RCM, generating thousands of dollars per-month in 2016 from AdDemand.

Another method of turning email into display advertising is to use fake search engines. Clicking a link inside an email will direct the recipient through a normal display advertising link and drop them onto a search results page, which displays ads as "search results" based on the topic of the email.

"Using the fake search engine trick is the most blatant way this is done. Yes, maybe the users are actually clicking on display ads presented within the fake search engine sites, but they are driven to those sites *only* through spam (nobody would just stumble across them accidentally). Even in this scheme, there are tracking codes embedded in every URL to ensure the correct spammers are getting paid for these so-called 'display advertising' clicks," Anderson added.

Other business ties for RCM, include Demand Media (Leaf Group LTD.), where RCM runs two BIND rotator servers, registered under Pheasant Valley Marketing and eBox Inc.

Between October 2016 and January 2017, RCM collected $937,451.21 USD for their campaigns from various affiliate networks, including AdDemand, W4, AD1 Media (Flex), and Union Square Media. RCM campaign logs show business relationships with some of these companies dating back to July of 2015.

Salted Hash reached out to Amobee comment. The company responded with a brief statement: "Amobee has ceased doing business with River City Media. We are committed to advertising standards that are in full compliance with all regulatory requirements."

This is not the end:

The River City Media data breach exposed so many records and other internals, there was just no way to fit everything into a single story. In the coming days and weeks, Salted Hash will continue following the money and business connections of the group and report on additional developments.

Head to Facebook to add your comments.

To comment on this article and other CSO content, visit our Facebook page or our Twitter stream.

Steve Ragan is senior staff writer at CSO. Prior to joining the journalism world in 2005, Steve spent 15 years as a freelance IT contractor focused on infrastructure management and security.

Follow

Healthcare records for sale on Dark Web

You Might Like